STATE OF ALABAMA

Information Technology Standard

Standard 670-07S1: Backup and Recovery

1. INTRODUCTION:

An important information system design and operational consideration is the ability to recover and restore data/information, should a problem occur. An integral part of ensuring security and integrity of the computing and network environment, and the availability of data, is a well-structured, documented, and tested backup and recovery program.

2. OBJECTIVE:

Establish requirements for backup and recovery of State of Alabama computing resources.

3. SCOPE:

These requirements apply to all users (State employees, contractors, vendors, and business partners) of any State of Alabama information system resources.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls, and recognized industry best business practices, the following standards shall apply to State backup and recovery operations:

4.1 INFORMATION SYSTEM BACKUP

Conduct backups of user-level and system-level information (including system state information) contained in the information system in accordance with data owner specifications and system security plans, and store backup information at an appropriately secured location.

Backup data shall be encrypted in accordance with State Standards.

System security plans shall include back-up and recovery program procedures that shall be tested at least twice annually. As a minimum, backup and recovery procedures shall provide the following:

- System configuration and hardware component descriptions
- Recovery prioritization
- Tested procedures for restoring the system
- Tested procedures for restoring and testing applications
- Tested procedures for restoring and verifying data from backup sources

The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) shall be based on the application, system, or data owner's recovery time and recovery point objectives.

4.2 ALTERNATE STORAGE SITES

Identify an alternate storage site and initiate necessary agreements to permit the storage and timely and effective recovery of information system backup information.

Alternate storage sites shall be geographically separated from the primary storage site so as not to be susceptible to the same hazards.

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

For mission-critical systems, store backup copies of the operating system and other critical information system software in a separate facility or in fire-rated containers that are not collocated with the operational software.

4.3 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Employ mechanisms with documented supporting procedures to allow the information system to be recovered and reconstituted to its original state after a disruption or failure.

Original state means all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, and the system is fully tested.

Include a full recovery and reconstitution of the information system as part of contingency plan testing.

Selectively use backup information in the restoration of information system functions as part of contingency plan testing.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 670-07: Backup and Recovery

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	12/12/2006	